

Benefits, Payroll and Retirement Operations

Health Insurance Portability & Accountability Act (HIPAA)



Table of Contents

	Page(s)
Definition	1
Overview	2 - 3
Health Information	4
Security & Privacy	5 - 6
Non-Compliance	6 - 7
Administration	8 - 13
Resources	14

Definition

Health Insurance Portability & Accountability Act (HIPAA)

The Health Insurance Portability & Accountability Act, commonly know as HIPAA, was passed by Congress in1996 to guarantee that individuals could move from one health plan to another without losing insurance coverage, or be denied coverage because of preexisting conditions.

HIPAA addresses these major healthcare issues:

- Portability the ability to transfer health insurance from one job to another
- Accountability the prevention of health care fraud and abuse

HIPAA Privacy Rule

HIPAA's Privacy Rules are designed to address the publics' concern for healthcare privacy. In addition to Protected Health Information (PHI), this includes Personal Identifier Information (PII) such as Social Security Numbers, birthdates, addresses and even zip codes. New technology increases privacy risk; e-mail, cell phones, Internet, etc.

- HIPAA creates national standards to protect PHI
- It also sets national boundaries on the use and release of health records
- Establishes appropriate safeguards for protection of PHI
- Strikes a balance to support disclosure for public health purpose
- Holds violators accountable Civil and Criminal Penalties
- HIPAA gives people the right to an accounting of how their PHI has been disclosed and to obtain a list of individuals and agencies that have received their PHI
- Limits releases to the minimum PHI necessary
- Empowers people to control some uses and disclosures of their protected health information.

HIPAA also gives individuals the right to:

- Obtain a copy of a his/her medical records
- Request correction of medical records
- File HIPAA complaints with King County and/or Office of Civil Rights
- Have reasonable requests for confidential information communications accommodated
- Determine who can have access to their PHI. For example, an employee can authorize BPROS to discuss healthcare needs with a spouse or domestic partner and vice versa.

Overview

Who is Covered

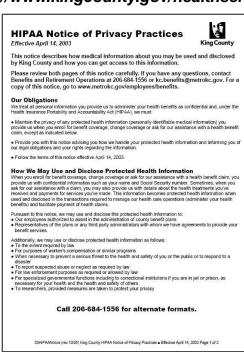
HIPAA requirements apply to:

- · Healthcare providers
- Health Plans Government and Private
- Healthcare Clearinghouse: A private or public entity that facilitates the transfer of health information from a non-standard format into a standard format or receives standard information and processes it into a non-standard format
- Business Associates Relationships: Entities that conduct business on behalf of King County
- Business Associate Subcontractors: All of the downstream entities that receive, access, maintain and/or disclose PHI

King County is considered a hybrid entity because it is both a **provider** and a **plan** by having departments that provide:

- Health & Mental Health care
- Administration of the King County healthcare plan
- Reimbursement or payments for health care services received

Below is the *HIPAA Notice of Privacy Practice*. The full document can be found in the Regular Employee New Hire Guide, pages 30-31. For further information, go to: http://www.kingcounty.gov/healthservices/MHSA/HIPAA/HIPAA/links.aspx



To business associates who provide services to us and assure us that they will protect the information from any unsubnoticed use of disclosure

I are not also as the control of the cont

Health Information

Health information is any information, whether verbal, recorded or electronic, in any form that:

- Is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearing house; and/or
- Relates to the past, present or future physical or mental health or condition of a individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual including demographic information.

Highly Sensitive Health Information

Highly Sensitive Health Information is considered any health information relating to:

- Testing for the Human Immunodeficiency Virus (HIV) or other sexually transmitted diseases.
- Treatment related to HIV or other sexually transmitted disease.
- Testing for cancer or other life-threatening illnesses.
- The diagnosis, treatment, or referral for treatment of a mental illness and/or alcohol or substance abuse.

Protected Health Information

Protected Health Information, or PHI, includes any health information, physical or mental health or condition of an individual, and any payment information for the provision of health care (includes demographic information) which either **specifically identifies the individual** it describes or **could be used to identify the individual**.

Within the scope of BPROS, PHI is any information obtained in the process of assisting employees with:

- Claims resolution
- · Claims processing
- Claims payment
- · Benefits enrollment information
- Processing payroll
- Processing W4 W2 information

Security and Privacy

Maintaining Protected Health Information

In order to maintain the security of protected health information, BPROS has developed administrative policies and procedures that comply with HIPAA.

For Example: PHI is logged into the secure EBMS Case Log by authorized BPROS staff only and paper copies are filed in locked file cabinets and maintained in a secure location accessible only to BPROS staff.

In addition, the Human Resources Division has developed disaster recovery plans and business continuation plans for the EBMS Case Log.

PHI Security

Providing quality customer service includes protecting employee's confidential healthcare information. First, because it is required by law, and second because it helps employee's trust administrative offices within the county.

HIPAA:

- Is required by Law
- Earns employee trust
- · Assures privacy of information
- Provides security of information
- Sets federal minimum standards and safeguards to protect PHI
- Preempts weaker state laws

As a King County employee, BA or subcontractor, you must be familiar with HIPAA policies and procedures so that you can show sensitivity and respect toward employees protected health and personal identifier information. You must respect each employee's right to privacy; treat all records as if they were your very own and be sensitive to privacy in all situations.

Inadvertent disclosures include all King County employees who may discuss or release PHI in the following situations:

- · Grocery stores, car pools, van pools or family time
- Discussion or answering questions in public areas such as hallways
- Jammed fax or copier machines left unattended
- Leaving sensitive information unattended on desks
- Revealing more than minimum information necessary in ANY situation.

Security & Privacy

PHI Access

King County staff may have access to protected health information whenever:

- An employee or vendor provides information to receive reimbursement or to get help with a claim.
- Employees send an "Explanation of Benefits" form to BPROS to get help with a claim.
- PHI is communicated between King County and a Third Party Administrator or a benefit vendor such as Group Health, Washington Dental Service and Vision Service Plan.
- Processing payroll.
- Communicating payroll transactions with external agencies. (leins, garnishments, etc.)

In cases of non-compliance, progressive discipline is based on the personnel system:

- Civil Service personnel may face sanctions up to and including termination from service
- Commissioned Officers may face sanctions to include recommendation for termination of commission.

In addition to the penalties that Civil Service and Commissioned Officers may face for violating HIPAA rules, all King County employees may be held *individually accountable* under the Privacy act.

Given the serious nature of PHI privacy, even *inadvertent* disclosure is considered a serious infraction. Deliberate <u>or</u> inadvertent disclosure of PHI for any reason may lead to discipline up to and including termination.

The Privacy Officer takes every precaution to train employees on HIPAA Privacy Rules and how to properly secure PHI.

Non-Compliance

Civil Penalties

Fines for civil infractions are enforced by the Office of Civil rights as follows:

Civil Monetary Penalties:

- \$100 Per Violation
- Capped at \$25,000 for each calendar year for each requirement of prohibition that is violated.

Criminal Penalties

The **criminal penalties** for HIPAA violations includes greater penalties for knowingly violating the rules. Also, HIPAA violations can be severe enough to be considered a **criminal** offense and carry the following fines and jail time:

- Up to \$50,000 Fine & 1 year imprisonment for knowingly obtaining or disclosing individually identifiable health information.
- Up to \$100,000 & 5 years imprisonment if done under false pretenses.
- Up to \$250,000 & 10 years imprisonment if done with intent to sell, transfer or use for commercial advantage, personal gain or malicious harm.
- Criminal penalties are enforced by U.S. Department of Justice.

Privacy Officer

Each King County department has a designated **Privacy Officer** or contact person who is responsible for developing policies and procedures for HIPAA compliance. The Privacy Officer also handles disclosure complaints and resolves HIPAA issues.

- Caroline Whalen is the Privacy Officer for DES, which includes the LEOFF Disability Board.
- Public Health, DCHS and the Sheriff's Office each have identified privacy officers.

Training

King County provides HIPAA training to all employees. New employees receive training no later than 30 days after beginning work. Training must also be provided when policies and procedures are revised. BA & Subcontractor training is provided as needed.

Staff training is documented and maintained in writing or electronically for six years.

King County has policies and procedures to safeguard PHI for both electronic and paper records. These safeguards include administrative, technical and physical safeguards:

Administrative Safeguards includes orientation and termination policies, incident reporting polices, access, contingency and disaster recovery.

Technical Safeguards: User access and restrictions, user monitoring, authentication and password issuance.

Physical Safeguards: Physical access control during and after hours, shredding policies and health record removal from facility.

In addition, BPROS has taken steps to avoid inadvertent disclosures and minimize violations including:

- Identifying gaps in securing data
- · Training, training and more training
- · Monitoring HIPAA case law

When the county becomes aware of a HIPAA violation or PHI disclosure, reasonable steps are taken to ensure minimizing of the disclosure or violation. Any inadvertent disclosure must be documented, maintained and filed, along with a brief explanation of the resolution of the complaint.

Individuals that disclose HIPAA violations are granted the same protections and rights as any other disclosures covered under the Whistleblower Protection Code of King County.

The county does not tolerate retaliations or intimidating actions against an individual that discloses HIPAA violations or for participating in any process established for:

- Filing complaints
- Testifying
- Assisting or participating in an investigation, compliance review, proceeding or hearing.

Also, the county cannot force individuals to waive their rights to file complaints under the HIPAA Privacy Rule.

Disclosure Tracking Form

When any PHI disclosure occurs, it must be reported *regardless* of if the disclosure was intentional or inadvertent.

Each BPROS team member is required to keep a **Disclosure Tracking Log**. This log is used to record any incidence of PHI disclosure that they have done, witnessed, or in any way been involved. The log is sent as needed or quarterly to the Privacy Officer who reviews the log and takes appropriate actions.

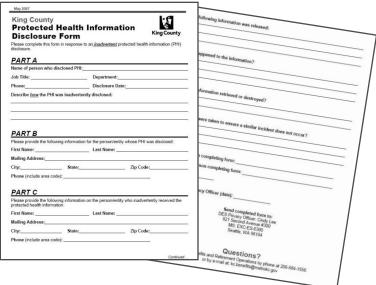
Below is a sample **Disclosure Tracking Log**. You need to complete this information any time you are party to or witness an inadvertent or intentional disclosure of PHI. This log is a companion piece to the **Disclosure Form** (next page). These forms are turned in to the Privacy Officer (Cindy Lee) on an as-needed basis or quarterly.

King County Protected Health II Disclosure Trackin	g Log	King County
II.	osures for treatment, payment and h	ealthcare operations Last Name:
l. Disclosure Date:	2	te: Zip Code;
Released To:	Last Name:	
		25
to the same and the same	tate: Zip Code:	
		Last Name:
Protected Health Information released:		
Reason for releasing information:		
Released By:		200 J (1999)
First Name:	Last Name:	Last Name:
2. Disclosure Date:		te: Zip Code:
Released To:		
First Name:	Last Name:	
Mailing Address:	50 08	
City: S	itate: Zip Code:	
		10
		lompleted Tracking Log to:
Released By:		1 Second Avenue #300
200 A C C C C C C C C C C C C C C C C C C	Last Name:	MS: EXC-ES-0300 Seattle, WA 98104
<u> </u>		

O

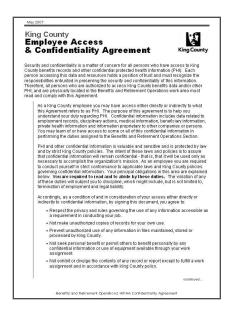
Disclosure Form

This is a sample of the **Protected Health Information Disclosure Form.** This is the form you would complete to report an *inadvertent* disclosure of protected health information.



Confidentiality Agreement

All BPROS staff (and certain other King County staff) must sign an annual **Confidentiality Agreement**. The agreement outlines the basic HIPAA rules and acknowledges that, as a county employee, you may have access to PHI. By signing the form, you are agreeing that you understand HIPAA and will abide by the policies, procedures and rules put in place by King County to secure protected health information.



е
vision,
tem eports
ition should
except

Allowable disclosures of PHI:

There are some circumstances in which PHI can legally be disclosed. These include:

- When there is a request for treatment or payment of claims for healthcare procedures.
- When required by law or for public health purposes, to comply with worker's compensation and similar laws.
- When there is a request from an individual to review his/her PHI. However, a
 person may not look at the medical records of an adult dependent without written
 permission.

For example: A husband may not have access to his wife's medical records <u>without her</u> <u>written consent</u>, however; a parent could have access to a child's' records if the child is **13 years old or under**.

King County	L. L. L.
Authorization	
Protected He	ealth Information KingCounty
(vour full name)	, authorize the disclosure and/or use of my protected
(your fill same) health information to:	
Company/Organization:	
First Name:	Last Name:
and the second s	- 1994 And September 1994 1
This authorization is valid fr	omtoe id date)
If no end date is indicated, thi	s authorization expires twelve (12) months from date signed.
The type of information to b	e disclosed (check all that apply):
Enrollment: Eligibility:	Claims: Other:
Furthermore:	ation to the King County Benefits and Retirement Operations Section sure my protected health information is voluntary.
	ise to sign this authorization.
• I may inspect or copy the in	nformation to be used or disclosed.
	osure carries with it the potential for unauthorized disclosure and protected by federal confidentiality rules.
Printed name of person con	npleting this form:
Signature of person comple	ting this form:
organicano or porconi compre	
Date:	
	Benefits and Retirement Operations Section Clafy Lee, Manager 82 (Second Are 114 # 500) MSC EXC-B-0000 0-edfte, (MA 99104 Prost: 205-654-1556

BPROS must have a current signed **Disclosure Request Form** on file in order to disclose PHI about a spouse/domestic partner or dependent to the employee, or vice versa.

E-mailing Protected Health Information

In the course of day-to-day business, it may be necessary for BPROS staff to e-mail PHI. As much as possible, e-mails containing PHI must be sent using the county's Voltage encryption software.

However, there are times when sending encrypted e-mail is not an option. For example: several King County vendors are not able to open encrypted e-mails. In this case, all available and reasonable precautions must be taken to protect the information.

The following steps outline the process for sending PHI via e-mail when encryption is not an option:

- Copy the PHI into a Microsoft Word document. If this is not possible, resave the document in its current program using the password protection guidelines in step two.
- 2. Save the Word document using the "password protect" feature.
- **3.** The password formula is the month (written out completely, initial capped) that the document was created.
- **4.** Send the password in a separate e-mail; never include the password with the protected information.

Although this method is not optimal, it does satisfy the HIPAA requirement by utilizing reasonable and available precautions in safeguarding PHI.

Alternatives

In addition to the rules, policies and procedures of protected health information, HIPAA grants individuals the right to request transmittal of PHI by **alternate means** or to an **alternate location**.

Alternate means are methods of sending confidential communications that are different from the usual methods. Usual methods are things like inter-office or U.S. mail. Alternate means would be e-mail, registered mail, hand-delivered, etc.

Alternate location means an address different from the mailing address. For example, the employee can ask to be contacted at work instead of at home or vice versa.

- The request must be submitted in writing and contain complete information about how the information will be sent, where the information is going and how it is to be addressed.
- The person making the request does not have to give a reason.
- The Benefits Manager or designee will approve or disapprove all requests. May only disapprove if request is not reasonable.
- Requests will be filed in the employee's benefits file after he/she has been notified of the decision of approval or disapproval.
- Above all, the request must be reasonable.

Resources

The following resources provide detailed information on HIPAA laws along with information on how King County abides by, and applies these laws. For specific questions about the county and HIPAA, contact the DES Privacy Officer, Caroline Whalen, via e-mail at: caroline.whalen@kingcounty.gov.

 King County Benefits Web Site http://www.kingcounty.gov/employees/benefits.aspx

King County Benefits Payroll & Retirement Operations

Phone: 206-684-1556

E-mail: kc.benefits@kingcounty.gov

 Whistleblower Protection Policy http://www.kingcounty.gov/operations/Ombudsman/whistleblower.aspx

 U.S. Department of Health & Human Services http://www.hhs.gov/ocr/hipaa/

U.S. Department of Justice

http://www.usdoj.gov/